Configuring BaySecure Firewall-1

BayRS Version 13.10
Site Manager Software Version 7.10

Part No. 117384-C Rev 00
November 1998

Bay Networks *Where Information Flows.*™

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1998 Bay Networks, Inc.

All rights reserved. Printed in the USA. November 1998.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FRE, LN, Optivity, PPX, Quick2Config, and Bay Networks are registered trademarks and Advanced Remote Node, ANH, ARN, ASN, BayRS, BaySecure, BayStack, BayStream, BCC, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, FN, IP AutoLearn, PathMan, RouterMan, SN, SPEX, Switch Node, System 5000, and the Bay Networks logo are trademarks of Bay Networks, Inc.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Bay Networks, Inc. ("Bay Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of

its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Before You Begin ix
Text Conventions x
Acronyms xi
Bay Networks Technical Publications xi
How to Get Help xii

Chapter 1
BaySecure FireWall-1

Managing Firewall Operation 1-1
How the Firewall Software Works 1-2
Where You Should Go from Here 1-2

Chapter 2
Installing FireWall-1 Management Software

Obtaining Software Licenses 2-1
Obtaining a FireWall-1 License for the Management Station 2-2
Sample Response from Check Point 2-3
Obtaining a FireWall-1 License for the Router 2-4
Sample Response from Check Point 2-5
Installing and Running the FireWall-1 Management Software 2-5
Installing on a Computer Running Windows NT 2-5
Sample Installation 2-6
Customizing the FireWall-1 Installation 2-12
Installing on a UNIX Platform 2-13
Before You Install 2-13
Mounting the CD and Extracting the Tar File 2-13
Installing the Check Point FireWall-1 Software 2-14
Installation Options 2-14
Sample Installation 2-14

Customizing the FireWall-1 Installation 2-18
Installing a License on the Management Station 2-19
Starting and Stopping the FireWall-1 Daemons 2-19
Synchronizing the Management Station and the Router Passwords 2-19
Starting FireWall-1 2-20
Transferring Security Policy and Configuration Files 2-20
Transferring Files from One PC to Another 2-20
Transferring Files from One UNIX or Windows NT Platform to Another 2-20

Chapter 3
Configuring a Firewall on a Router

Creating a Firewall on the Router 3-1
Using Site Manager 3-2
Disabling or Reenabling the Firewall on the Router 3-4
Setting Up Communications Between the Firewall Management Station and the Router 3-4
Establishing a Static Route 3-4
Establishing the Firewall Management Station 3-5
Identify the First Backup Firewall Management Station 3-6
Identify the Second Backup Firewall Management Station 3-7
Identifying the Router 3-8
Enabling the Firewall on Router Interfaces 3-8
Activating the Firewall 3-12
Defining a Firewall Security Policy 3-13
Installing the Security Policy on the Router and Its Interfaces 3-14
Deleting Firewall from the Router 3-15
Deleting Firewall Locally or Remotely Using Site Manager 3-15
Deleting Firewall Dynamically Using the Technician Interface 3-16
Troubleshooting Checklist 3-17

Appendix A
Parameter Descriptions

FireWall Enable Parameter A-1
FireWall Parameters A-2
List FireWall Interfaces Parameters A-4

Index

Figures

Figure 2-1. Choose Destination Location Window 2-6
Figure 2-2. Selecting Product Type Window 2-7
Figure 2-3. Licenses Window 2-8
Figure 2-4. Administrators Window 2-9
Figure 2-5. Add Administrators Window 2-9
Figure 2-6. Key Hit Session Window 2-10
Figure 2-7. Choose Destination Location Window 2-11
Figure 2-8. Select Components Window 2-12
Figure 3-1. Configuration Manager Window 3-2
Figure 3-2. Create Firewall Dialog Box 3-3
Figure 3-3. List Firewall Interfaces Window 3-10
Figure 3-4. Values Window 3-11
Figure 3-5. Boot Router Window 3-12

Preface

This guide describes BaySecure FireWall-1 and what you do to install, start and customize BaySecure FireWall-1 services on a Bay Networks® router.

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (see the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Bay Networks BayRS™ and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is: **ping <***ip_address***>**, you enter: **ping 192.32.10.12**
bold text	Indicates command names and options and text that you need to enter. Example: Enter **show ip** {**alerts** | **routes**}. Example: Use the **dinfo** command.
braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you must enter either: **show ip alerts** or **show ip routes**, but not both.
italic text	Indicates file and directory names, new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is: **show at <***valid_route***>** *valid_route* is one variable and you substitute one value for it.
`screen text`	Indicates system output, for example, prompts and system messages. Example: `Set Bay Networks Trap Monitor Filters`

separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you enter either: **show ip alerts** or **show ip routes**, but not both.

Acronyms

GUI	graphical user interface
IP	Internet Protocol
LAN	local area network
MIB	management information base
ISO	International Organization for Standardization
TCP/IP	Transmission Control Protocol/Internet Protocol

Bay Networks Technical Publications

You can now print Bay Networks technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the Bay Networks product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

You can purchase Bay Networks documentation sets, CDs, and selected technical publications through the Bay Networks Collateral Catalog. The catalog is located on the World Wide Web at *support.baynetworks.com/catalog.html* and is divided into sections arranged alphabetically:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

Make a note of the part numbers and prices of the items that you want to order. Use the “Marketing Collateral Catalog description” link to place an order and to print the order form.

How to Get Help

For product assistance, support contracts, information about educational services, and the telephone numbers of our global support offices, go to the following URL:

http://www.baynetworks.com/corporate/contacts/

In the United States and Canada, you can dial 800-2LANWAN for assistance.

Chapter 1
BaySecure FireWall-1

BaySecure™ FireWall-1 builds firewall security features into Bay Networks router software. It does this by integrating the stateful inspection module from Version 2.1 of the Check Point Software Technologies FireWall-1 software into the Bay Networks router operating system of Bay Networks BN®, ASN™ and ARN™ routers. BaySecure FireWall-1 provides all of the security features from Version 2.1 of the Check Point Software Technologies FireWall-1 software, except for user authentication, address translation, statistics and encryption.

Managing Firewall Operation

A *firewall* is the hardware and/or software that limits the exposure of a computer or network to an invasion from an external source. To control the operation of a firewall on the router, you use the Check Point FireWall-1 management software.

You install this management software on a computer running Windows NT or UNIX to create a *firewall management station*. From the management station, you can use the FireWall-1 management software to define a security policy and download it to the router. The *security policy* specifies how the firewall operates. For instructions on how to install the FireWall-1 management software, see Chapter 2, “Installing FireWall-1 Management Software.” To learn how to configure a security policy, see your Check Point documentation.

How the Firewall Software Works

The *stateful inspection module* in the Bay Networks router software inspects all data packets traveling between the data link and network layers, and communicates the results to the management station. If the data packets meet the security requirements specified in the security policy, the router forwards the data. If the data packets violate the security policy, the router drops the data packets, and logs the information to the management station.

Where You Should Go from Here

To get a firewall up and running on your Bay Networks router:

For information on how to	Go to page
Obtain licenses from Check Point	2-1
Install the Check Point Management software	2-5
Create a firewall	3-1
Enable the firewall on the router	3-8
Establish a relationship between the management station and the router	3-4
Enable the router on specific interfaces	3-8
Activate the firewall	3-12
Configure a firewall security policy	3-13, and see your Check Point FireWall-1 documentation
Install the security policy on the router	3-14, and see your Check Point FireWall-1 documentation

Chapter 2
Installing FireWall-1 Management Software

To install the FireWall-1 software, see the following sections:

Topic	Page
Obtaining Software Licenses	2-1
Installing and Running the FireWall-1 Management Software	2-5

Obtaining Software Licenses

Before you can install the FireWall-1 software and create a firewall on the router, you must first obtain a permanent software license from Check Point Software Technologies for:

- The firewall management station

  You need one software license for the firewall management station, a PC or UNIX workstation used to manage the firewall software on the Bay Networks router. You also need a software license for each backup management station that you configure.

- The router

  You need one software license for each Bay Networks router protected by the firewall software.

Obtaining a FireWall-1 License for the Management Station

To obtain a FireWall-1 license for the firewall management station, follow these instructions:

Note: You need one license for each FireWall-1 management station. To obtain a license for each additional management station, you must repeat the steps outlined in this section.

1. **Locate your certificate key.**

   A certificate key (serial number) is located on a sticker on the inside of the CD folder containing the Check Point FireWall-1 management software media. If you lose the certificate key bearing the FireWall-1 serial number, contact Bay Networks.

2. **Contact Check Point Software Technologies.**

   To obtain a permanent license, you must contact Check Point with your certificate key information. You can reach Check Point in any of these ways:

   - On the World Wide Web at *http://license.CheckPoint.com*
   - By sending e-mail to license@checkpoint.com
   - By phoning Check Point:

     800-429-4391 (North America)

     +972-3-613-1833 (outside North America)

   When requesting a license, you must also be prepared to provide the IP address of the management station on which you plan to install the license.

Sample Response from Check Point

```
Your license request with the following details has been accepted.
Below you will find the corresponding license string.

We recommend printing this page and saving it in your files for future
reference.

Request Details
---------------
Certificate Key:    5xxx 5xxx fxxx
Customer Name:      Bay Networks
Product:            CPFW-ESC-U
Version:            3.0
Host ID:            123.123.123.123

License(s) Issued
-----------------
Host ID:            123.123.123.123
Features:           control
License String:     7xxxxxxx-8xxxxxxx-fxxxxxxx

License(s) Installation
-----------------------
run 'fw putlic 123.123.123.123 7xxxxxxx-8xxxxxxx-fxxxxxxx control '

Contact Information
-------------------
This Check Point product has been purchased through: Bay Networks
```

Note: If you need to change the IP address of a FireWall-1 management station, contact Check Point at 800-429-4391 (North America) or +972-3-613-1833 (locations outside of North America).

For information about how to install the license, refer to the section "Installing and Running the FireWall-1 Management Software" on page 2-5 and the Check Point FireWall-1 documentation.

Obtaining a FireWall-1 License for the Router

To obtain a FireWall-1 license for a router you plan to protect with a firewall, follow these instructions:

Note: You need one license for each router that you plan to protect with a firewall. To obtain a license for each additional router, you must repeat the steps outlined in this section.

1. **Locate your certificate key.**

   A certificate key (serial number) is located on a sticker on the inside of the CD folder containing the Check Point FireWall-1 software media. If you lose the certificate key bearing the FireWall-1 serial number, contact Bay Networks.

2. **Contact Check Point Software Technologies.**

   To obtain a permanent license, you must contact Check Point. To process your request, Check Point requires your certificate key and the IP address of the router you plan to protect with a firewall.

   You can reach Check Point in any of these ways:

   - On the World Wide Web at *http://license.CheckPoint.com*
   - By sending e-mail to license@checkpoint.com
   - By phoning Check Point:

     800-429-4391 (North America)

     +972-3-613-1833 (outside North America)

   To synchronize the FireWall-1 password on the router and the management station, use the **fw putkey** command. See "Synchronizing the Management Station and the Router Passwords" on page 2-19.

Sample Response from Check Point

```
The following license was generated:
We recommend printing this page and saving it in your files for future
reference.

Request Details
---------------
Certificate Key:    7xxx dxxx 1xxx
Customer Name:      Bay Networks
Product:            BABN-IM-U
Version:            3.0
Host ID:            012.012.012.012

License Issued
--------------
Host ID:            012.012.012.012
Features:           embedul
License String:     7fff6161-408d3b21-a161c10f

License Installation
--------------------
run 'fw putlic 012.012.012.012 7fff6161-408d3b21-a161c10f embedul '
```

Installing and Running the FireWall-1 Management Software

Once you obtain a FireWall-1 license from Check Point, you can install the Check Point FireWall-1 management software on a computer running either Windows NT or UNIX.

Topic	Page
Installing on a Computer Running Windows NT	2-5
Installing on a UNIX Platform	2-13

Installing on a Computer Running Windows NT

Use the following sections as a guide to installing the FireWall-1 management software on a computer running Windows NT. For more details, refer to your Check Point FireWall-1 documentation.

Sample Installation

The following sample installation takes the Check Point FireWall-1 software from a CD and installs it onto a PC running Windows NT. Use this sample installation to familiarize yourself with a basic FireWall-1 installation.

Note: This sample installation shows only those screens necessary for a basic installation. Your installation may be different.

Installing the Management Software

1. **Insert the CD into the CD-ROM drive and run the Setup program, *setup.exe*. To specify the name and location of the program to run, enter (where D is the name of your CD-ROM drive):**

   D:\windows\fw1\setup.exe

   The Choose Destination Location window (Figure 2-1) opens.

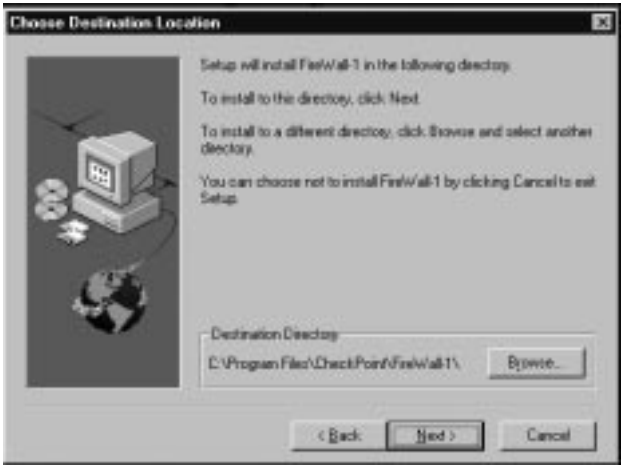
Choose Destination Location
Setup will install FireWall-1 in the following directory.
To install to this directory, click Next.
To install to a different directory, click Browse and select another directory.
You can choose not to install FireWall-1 by clicking Cancel to exit Setup.
Destination Directory
C:\Program Files\CheckPoint\FireWall-1\
Browse...
< Back
Next >
Cancel

Figure 2-1. Choose Destination Location Window

2. **Choose a destination directory. You can either accept the default directory (Program Files) or make another selection.**
3. **Click on Next.**

The Selecting Product Type window (Figure 2-2) opens.

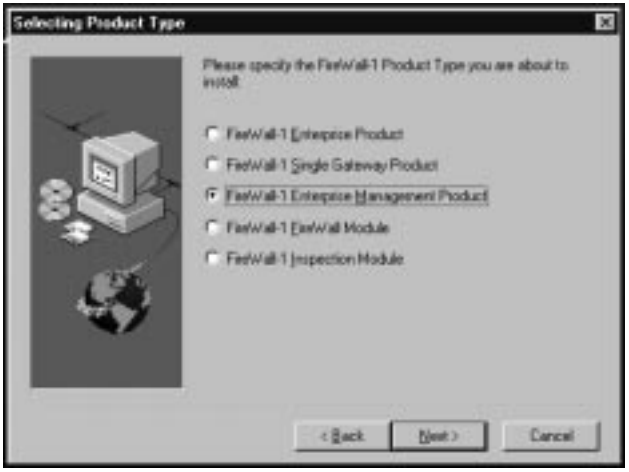
Selecting Product Type
Please specify the FireWall-1 Product Type you are about to install.
FireWall-1 Enterprise Product
FireWall-1 Single Gateway Product
FireWall-1 Enterprise Management Product
FireWall-1 FireWall Module
FireWall-1 Inspection Module
< Back
Next >
Cancel

Figure 2-2. Selecting Product Type Window

4. **Choose the FireWall-1 component you want to install. To be compatible with BaySecure FireWall-1, choose FireWall-1 Enterprise Management Product.**

5. **Click on Next.**

   The Licenses window (Figure 2-3) opens.

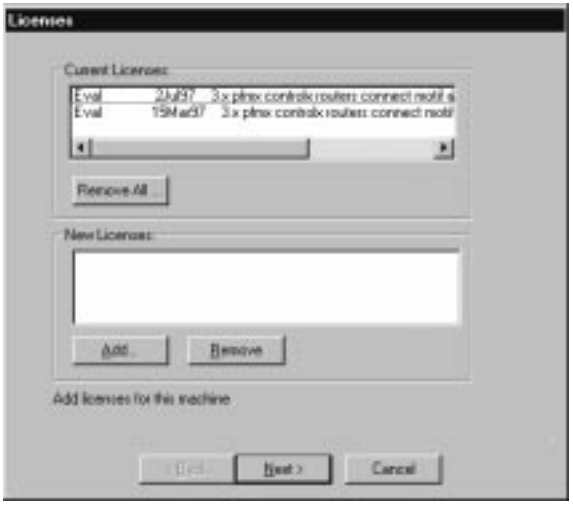

Figure 2-3. Licenses Window

6. **Enter the license information you obtained from Check Point.**

7. **Click on Next.**

   The Administrators window (Figure 2-4) opens.

Figure 2-4. Administrators Window

   You must specify at least one administrator.

8. **Click on Add.**

   The Add Administrator window (Figure 2-5) opens.

Figure 2-5. Add Administrators Window

9. **Enter the administrator's user name and password (limited to eight characters), and a password confirmation, then click on OK. You return to the Administrators window.**

10. **Click on Next.**

    The GUI Clients window opens. Do not enter any GUI clients at this time.

11. **Click on Next.**

    The Remote Modules window appears. Do not enter any remote modules at this time.

12. **Click on Next.**

    The Key Hit Session window (Figure 2-6) opens.

Figure 2-6. Key Hit Session Window

13. **Follow the directions in the window and enter random characters, with a delay of a few seconds between them, until the indicator bar is full.**

    Be sure not to type the same character twice in a row, to vary the delay between the characters.

14. **Click on Next.**

    The CA Key window opens.

15. **Click on Generate to generate a new key.**

    The host uses the RSA key to generate a digital signal for authenticating its communications in its capacity as a Certificate Authority.

    Generating the key may take several minutes.

16. **Click on Finish.**

Installing the GUI Client

1. **Insert the CD into the CD-ROM drive and run the *setup.exe* file. To specify the name and location of the program to run, enter (where D is the name of your CD-ROM drive):**

   D:\windows\gui_client\disk1\setup.exe

   The Choose Destination Location window (Figure 2-7) opens.

2. **Choose a destination directory.**

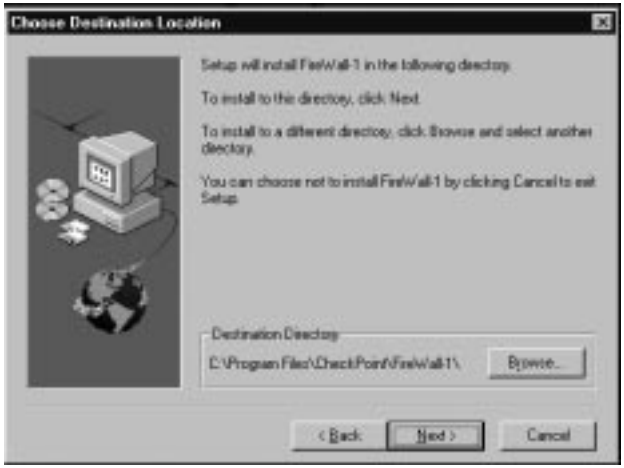
Choose Destination Location
Setup will install FireWall-1 in the following directory.
To install to this directory, click Next.
To install to a different directory, click Browse and select another directory.
You can choose not to install FireWall-1 by clicking Cancel to exit Setup.
Destination Directory
C:\Program Files\CheckPoint\FireWall-1\
Browse...
< Back
Next >
Cancel

Figure 2-7. Choose Destination Location Window

You can either accept the default directory (Program Files) or make another selection.

3. **Click on Next.**

   The Select Components window (Figure 2-8) opens.

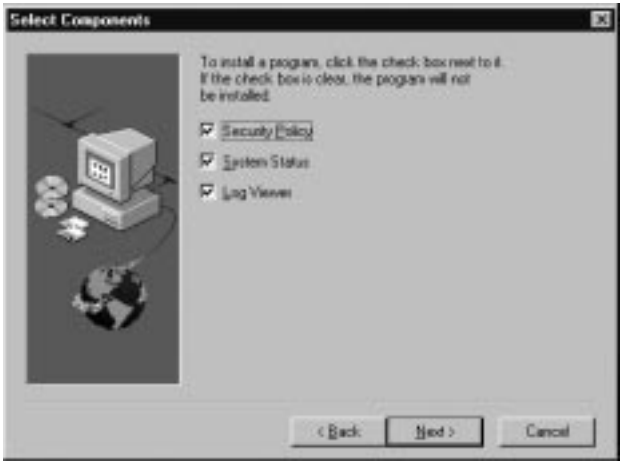
Select Components
To install a program, click the check box next to it. If the check box is clear, the program will not be installed.
Security Policy
System Status
Log Viewer
< Back
Next >
Cancel

Figure 2-8. Select Components Window

4. **Install the Security Policy, System Status, and Log Viewer components by clicking on each item.**

Customizing the FireWall-1 Installation

You can customize your FireWall-1 installation by running the *FireWall-1 Configuration* file.

To execute the file, enter:

D:\Start\Programs\FireWall-1\FireWall-1 Configuration

Using the *FireWall-1 Configuration* file, you can add:

- A license
- Administrators
- GUI clients
- Remote modules
- CA keys

For more information, refer to your Check Point documentation.

Installing on a UNIX Platform

Use the following sections as a guide to installing the FireWall-1 software on a computer running UNIX. For more details, refer to your Check Point FireWall-1 documentation.

Before You Install

Before you attempt to install the Check Point FireWall-1 software, be sure that you have completed these tasks:

- Obtain a FireWall-1 license for each firewall management station and router that you plan to protect with a firewall.
- Add **setenv FWDIR/etc/fw** to your *.cshrc* file, or add **FWDIR=/etc/fw** to your *.cshrc* file and, if using the korn shell, add **export FWDIR** to your *.profile* file; if using the c shell, add **setenv FWDIR** to your *.profile* file.
- Add **/etc/fw/bin** to your path.
- Add **/etc/fw/man** to your MANPATH environment.

Mounting the CD and Extracting the Tar File

Check Point distributes its FireWall-1 software on CD-ROM. You must supply the UNIX commands to mount the CD drive and extract the tar files.

The commands to mount a CD drive and extract the tar files vary depending on the device name of the CD drive, the operating system used, and other environmental factors. Use the instructions that follow only as guidelines for mounting the CD drive and extracting the tar files. The commands you need may differ.

For SunOS

```
lab#  mount -r -t hsfs /dev/sr0 /cdrom
lab#  cd /tmp
lab#  tar xvf /cdrom/sunos4/fw1/fw.sunos4.tar
```

For Solaris

```
lab#  mount -F hsfs -r /dev/sr0 /cdrom
lab#  cd /tmp
lab#  tar xvf /cdrom/solaris2/fw1/fw.solaris2.tar
```

For HPUX

```
lab#   mount -r /dev/dsk/c1t2d0 (or your specific CD-ROM address)  /cdrom
lab#   cd /tmp
lab#   tar xvf  "/cdrom/HPUX/FW1/FW.HPUX.TAR;1"
```

Installing the Check Point FireWall-1 Software

Once you have extracted the Check Point FireWall-1 files, you can install the management software. To install the software, change directories so that you're in the directory where you put the extracted files and then issue the **fwinstall** command.

For example, if you extracted the files into your */tmp* directory, install the software by entering the following commands:

```
lab#   cd /tmp
lab#   ./fwinstall
```

Installation Options

Note that during the installation, the script asks you to select the FireWall-1 option you want to install. To be compatible with BaySecure FireWall-1, enter selection 3, FireWall-1 Enterprise Management Console Product. A sample follows.

```
Which of the following FireWall-1 options do you wish to install?

(1) FireWall-1 Enterprise Product
(2) FireWall-1 Single Gateway Product
(3) FireWall-1 Enterprise Management Console Product
(4) FireWall-1 FireWall Module
(5) FireWall-1 Inspection Module

Enter your selection (1-7/a): 3
```

Sample Installation

The following sample installation takes the Check Point FireWall-1 software from a CD and installs it onto a SparcStation running SunOS. Use this sample installation to familiarize yourself with the FireWall-1 installation script.

Note: In the following sample installation, all user input is in **bold**.

```
**************** FireWall-1 v3.0 Installation ****************

Reading fwinstall configuration.  This might take a while.
Please wait.

Configuration loaded.  Running FireWall-1 Setup.

Checking available options. Please wait.....................

Which of the following FireWall-1 options do you wish to install/
configure ?
------------------------------------------------------------------
-----
(1) FireWall-1 Enterprise Product
(2) FireWall-1 Single Gateway Product
(3) FireWall-1 Enterprise Management Console Product
(4) FireWall-1 FireWall Module
(5) FireWall-1 Inspection Module

Enter your selection (1-5/a): 3

Installing/Configuring FireWall-1 Enterprise Management Console
Product.

Please wait...

Selecting where to install FireWall-1
--------------------------------------
FireWall-1 requires approximately 9017 KB of free disk space.
Additional space is recommended for logging information.

Enter destination directory [/etc/fw]): <Return>

Checking disk space availability...

Installing FW under /etc/fw (50836 KB free)
Are you sure (y/n) [y] ? y

Software distribution extraction
--------------------------------
Extracting software distribution. Please wait ...
Software Distribution Extracted to /etc/fw
Installing license
------------------
Reading pre-installed license file fw.LICENSE... done.
```

```
The following evaluation License key is provided with this
FireWall-1 distribution
Eval            15Mar97    3.x pfmx controlx routers connect motif

Do you want to use this evaluation FW-1 license (y/n) [y]? n

Do you wish to start FireWall-1 automatically from /etc/rc.local
(y/n) [y] ? n


Welcome to FireWall-1 Configuration Program
===========================================
This program will guide you through several steps where you
will define your FireWall-1 configuration. In any later time,
you can reconfigure these parameters by running fwconfig


Configuring Licenses...
=======================
The following licenses are installed on this host:
Eval            15Mar97    3.x pfmx controlx routers connect motif

Do you want to add licenses (y/n) [n] ? n

Configuring Administrators...
=============================
No FireWall-1 Administrators are currently defined for this
Management Station.

Do you want to add users (y/n) [y] ? n


Configuring GUI clients...
==========================
GUI clients are trusted hosts from which FireWall-1 Administrators
are
allowed to log on to this Management Station using Windows/X-Motif
GUI.

Do you want to add GUI clients (y/n) [y] ? n

Configuring Remote Modules...
=============================
Remote Modules are FireWall or Inspection Modules that are going
to be controlled by this Management Station.

Do you want to add Remote Modules (y/n) [y] ? n
```

```
Configuring Groups...
=====================
FireWall-1 access and execution permissions
-------------------------------------------
Usually, FireWall-1 is given group permission for access and
execution.
You may now name such a group or instruct the installation
procedure
to give no group permissions to FireWall-1. In the latter case,
only the
Super-User will be able to access and execute FireWall-1.

Please specify group name [<RET> for no group permissions]:

No group permissions will be granted. Is this ok (y/n) [y] ? y

Configuring Random Pool...
==========================
You are now asked to perform a short random keystroke session.
The random data collected in this session will be used for
generating Certificate Authority RSA keys.

Please enter random text containing at least six different
characters. You will see the '*' symbol after keystrokes that
are too fast or too similar to preceding keystrokes. These
keystrokes will be ignored.

Please keep typing until you hear the beep and the bar is full.

    [                   ] *

Thank you.

Configuring CA Keys...
======================
fw: no license for 'ca'
The installation procedure is now creating an FWZ Certificate
Authority Key
for this host. This can take several minutes. Please wait...
fw: no license for 'ca'

Configuration ended successfully

*************** FireWall-1 is now installed. ***************

Do you wish to start FW-1 now (y/n) [y] ? n
****************************************************************
Configuration ended successfully
```

```
*************** FireWall-1 is now installed. ***************

Do you wish to start FW-1 now (y/n) [y] ? n

*****************************************************************
                DO NOT FORGET TO:
1. add the line:    setenv FWDIR /etc/fw   to .cshrc
                or  FWDIR=/etc/fw; export FWDIR to .profile
2. add  /etc/fw/bin  to path
3. add  /etc/fw/man  to MANPATH environment
*****************************************************************

You may configure FireWall-1 anytime, by running fwconfig.

*************** Installation completed successfully *************
```

Customizing the FireWall-1 Installation

You can use the **fwconfig** command to customize your FireWall-1 installation. Using **fwconfig**, you can add or remove:

- A license
- Administrators
- Groups
- GUI clients
- Remote modules
- CA keys

Note: To add an administrator, you must first add a group in which the user is a member. If you do not add a group, then you can run the FireWall-1 GUI using only the **fwui** command if you are logged in as root.

For more detail, refer to your Check Point FireWall-1 documentation.

Installing a License on the Management Station

To install a license on the firewall management station, use the following command:

fw putlic *<hostid> <lic_string>* **pfmx controlx routers motif embedded**

The *hostid* is the host ID of the management station.

The *lic_string* is a string of alphanumeric characters that Check Point provides with your FireWall-1 license.

Starting and Stopping the FireWall-1 Daemons

To *start* the FireWall-1 daemons, use the **fwstart** command. For example, at the system prompt, enter:

```
lab# fwstart
```

To *stop* the FireWall-1 daemons, use the **fwstart** command. For example, at the system prompt, enter:

```
lab# fwstop
```

Synchronizing the Management Station and the Router Passwords

Once you have installed licenses on the firewall management station and the router, you must synchronize your password on the two systems. To synchronize the router and the management station passwords, enter the following commands:

- On the firewall management station:

  fw putkey -p*<password> <ip_address_fwall_router>*

- On the router:

  fwputkey <*password> <ip_address_mgmt_station>*

Where	Is
<password>	A string of alphanumeric characters that specifies your password
<ip_address_fwall_router>	The IP address of your firewalled router
<ip_address_mgmt_station>	The IP address of your FireWall-1 management station

Starting FireWall-1

To start FireWall-1, enter the **fwui&** command. For example, at the system prompt, enter:

```
lab# fwui&
```

Optionally, you can use the FireWall-1 XMotif graphical user interface. For instructions on how to install and start the XMotif GUI, see you Check Point documentation.

Transferring Security Policy and Configuration Files

Firewall backup management stations must have the same security policies and configuration files that the primary firewall management station uses. You can use the **fwfilex** command to transfer security policies and configuration files from one PC to another or from one UNIX or Windows NT platform to another.

Transferring Compressed Files from One PC to Another

When using the **fwfilex** command to transfer compressed files between PCs running Windows 95, the *zip.exe, unzip.exe*, and *fwfilex.cmd* files must be located in the FireWall-1 bin directory (typically *\WINNT\FW1\bin*).

To transfer compressed files between PCs, follow these steps:

1. Enter **fwfilex -i** *<filename>* to compress the files before you transfer them. This command produces a file called *<filename>.zip*.
2. Copy *<filename>.zip* to the FireWall-1 bin directory on the destination machine.
3. On the destination machine, uncompress the files by entering **fwfilex -o** *<filename>*.**zip**

Transferring Files from One UNIX or Windows NT Platform to Another

When using the **fwfilex** command to transfer files between machines running UNIX or Windows NT, you must set the FWDIR variable (typically to */etc/fw*) and you must set the permissions so that you have write privilege to the FWDIR directories. The transfer file, *fwfilex*, must reside in the *FWDIR/bin* directory (typically */etc/fw/dir*).

To transfer files between between machines running UNIX, follow these steps:

1. Enter **fwfilex -i** *<filename>*.**tar** to compress the files before you transfer them. This command produces a file called *<filename>.tar*.
2. Copy *<filename>.tar* to the FireWall-1 bin directory on the destination machine.
3. On the destination machine, uncompress the files by entering **fwfilex -o** *<filename>*.**tar**

Chapter 3
Configuring a Firewall on a Router

To configure a firewall on the router, see the following topics:

Topic	Page
Creating a Firewall on the Router	3-1
Disabling or Reenabling the Firewall on the Router	3-4
Setting Up Communications Between the Firewall Management Station and the Router	3-4
Enabling the Firewall on Router Interfaces	3-8
Activating the Firewall	3-12
Defining a Firewall Security Policy	3-13
Installing the Security Policy on the Router and Its Interfaces	3-14
Deleting Firewall from the Router	3-15
Troubleshooting Checklist	3-17

Creating a Firewall on the Router

Before you can create a firewall on the router, you must first configure and enable IP on the router and enable TCP on all slots on the router. For instructions, see *Quick-Starting Routers*.

This section explains how to create a firewall on a Bay Networks router using Site Manager.

You can also use the Technician Interface, which lets you modify parameters by issuing **set** and **commit** commands that specify the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: Unlike using Site Manager, the Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

Using Site Manager

Begin by starting Site Manager. Then follow these steps:

1. **Select Configuration Manager in either local, remote, or dynamic mode from the Tools menu.**

   The Configuration Manager window opens (Figure 3-1).

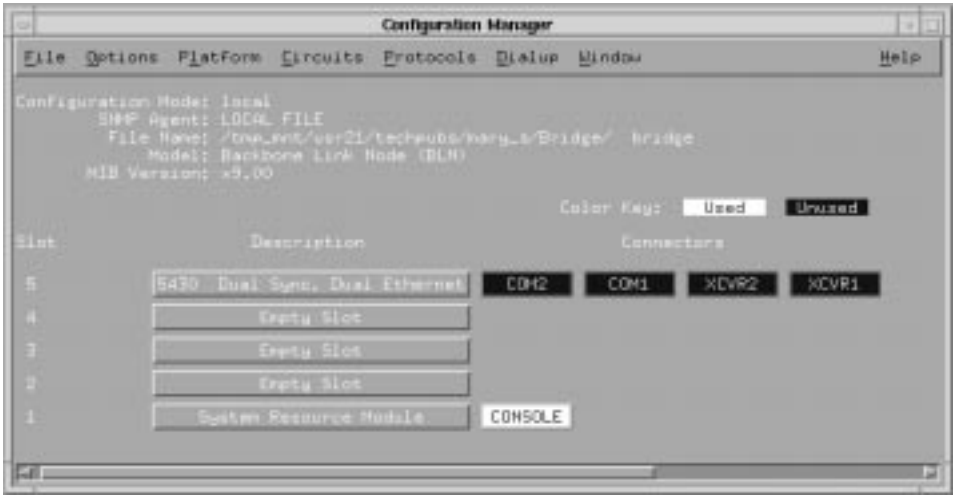

Figure 3-1. Configuration Manager Window

2. **If local or remote mode is selected, open a configuration file.**

3. Create a firewall by completing the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. From Configuration Manager, choose **Platform**.	The Platform menu opens.
2. Choose **FireWall**.	The FireWall menu opens.
3. Choose **Create**.	A dialog box opens. See Figure 3-2.
4. Click on **OK**	You return to the Configuration Manager window.

By default, the firewall is automatically enabled on the router. To disable or reenable the firewall, see "Disabling or Reenabling the Firewall on the Router" on page 3-4.

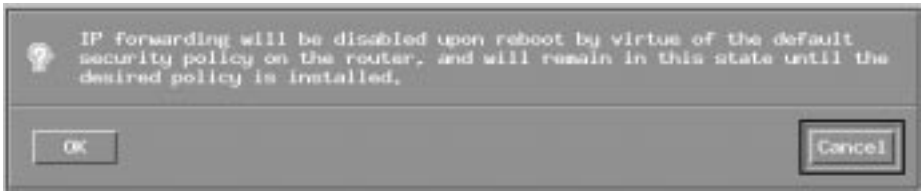
IP forwarding will be disabled upon reboot by virtue of the default security policy on the router, and will remain in this state until the desired policy is installed.
OK
Cancel

Figure 3-2. Create Firewall Dialog Box

Disabling or Reenabling the Firewall on the Router

By default, a firewall is enabled when you first create it on the router. To disable or reenable a firewall, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. From Configuration Manager, choose **Platform.**	The Platform menu opens.
2. Choose **FireWall**.	The FireWall menu opens.
3. Choose **Global.**	The FireWall Enable window opens.
4. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-1.	
5. Click on **OK**.	You return to the Configuration Manager window.

Setting Up Communications Between the Firewall Management Station and the Router

The firewall cannot protect your router until you set up communications between the firewall management station and the router. You must also establish the relationship between each backup firewall management station and the firewall management station it supports

To establish these relationships, you must use the same IP address you used to obtain FireWall-1 licenses for the router and each firewall management station.

Establishing a Static Route

You may need to establish a static route between the router and the management station before you configure the firewall parameters. By default, FireWall-1 filters in-bound routing protocol packets from RIP or OSPF. Therefore, if your router and firewall management station are on different subnets, you will need to establish a static route on the router, pointing to the management station's subnet; otherwise, your management station will be unable to communicate with the router. For information about creating a static route, see *Configuring IP Services.*

Establishing the Firewall Management Station

The firewall management station is the PC or UNIX workstation where you installed the FireWall-1 software. You use the firewall management station to enforce the firewall security policy that you created for the router. The management station also logs all attempted violations of the security policy. (To define a security policy, see "Defining a Firewall Security Policy" on page 3-13. You will also need to consult your Check Point FireWall-1 documentation.)

To identify the management station to the router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. From Configuration Manager, choose **Platform**.	The Platform menu opens.
2. Choose **FireWal**l.	The FireWall menu opens.
3. Choose **FireWall Parameters**.	
4. Set the **Log Host Address** parameter. Click on **Help** or see the parameter description on page A-2.	
5. Click on **Apply**.	The FireWall Parameters window remains open.
6. Click on **OK**.	You return to the Configuration Manager window.

Identify the First Backup Firewall Management Station

If your router loses communication with its firewall management station, the first backup firewall management station automatically establishes communication with the router so that the firewall security remains intact.

To identify the first backup firewall management station, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. From Configuration Manager, choose **Platform**.	The Platform menu opens.
2. Choose **FireWall**.	The FireWall menu opens.
3. Choose **FireWall Parameters**.	A dialog box opens. See ““Establishing a Static Route” on page 3-4.”
4. Click on **OK**.	The FireWall Parameters window opens.
5. Set the **Log Host Backup 1** parameter. Click on **Help** or see the parameter description on page A-2.	
6. Click on **Apply**.	The FireWall Parameters window remains open.
7. Click on **OK**.	You return to the Configuration Manager window.

Identify the Second Backup Firewall Management Station

If your router loses communication with its firewall management station and the first backup firewall management station, the second backup firewall management station automatically establishes communication with the router so that the firewall security remains intact.

To identify the tertiary firewall management station, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. From Configuration Manager, choose **Platform**.	The Platform menu opens.
2. Choose **FireWall**.	The FireWall menu opens.
3. Choose **FireWall Parameters**.	A dialog box opens. See ““Establishing a Static Route” on page 3-4.”
4. Click on **OK**.	The FireWall Parameters window opens.
5. Set the **Log Host Backup 2** parameter. Click on **Help** or see the parameter description on page A-3.	
6. Click on **Apply**.	The FireWall Parameters window remains open.
7. Click on **OK**.	You return to the Configuration Manager window.

Identifying the Router

To identify the router protected by the firewall, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. From Configuration Manager, choose **Platform**.	The Platform menu opens.
2. Choose **FireWall**.	The FireWall menu opens.
3. Choose **FireWall Parameters**.	The FireWall Parameters window opens.
4. Set the **Local Interface IP Address** parameter. Click on **Help** or see the parameter description on page A-3.	
5. Click on **OK**.	You return to the Configuration Manager window.

Enabling the Firewall on Router Interfaces

After you have created a firewall on the router, you can enable it on one or more interfaces.

To enable a firewall on one or more router interfaces, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. From Configuration Manager, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP.**	The IP menu opens.
3. Choose **FIREWALL**.	The List FireWall Interfaces window opens. See Figure 3-3 on page 3-10.
4. Click on **Add**.	The Values window opens. See Figure 3-4 on page 3-11.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Click on **All** to display all router interfaces or choose a *connection button* to display router interfaces by connection type.	Site Manager lists the interfaces at the top of the screen.
6. Click on **Check All** to highlight all listed interfaces, or highlight individual interfaces.	
7. Click on **OK**.	Site Manager returns you to the List FireWall Interfaces window. See Figure 3-3.
8. Set the FireWall **Name** parameter for the highlighted interface. Click on **Help** or see the parameter description on page A-4.	
9. Set the **Disable** parameter. Click on **Help** or see the parameter description on page A-4.	
10. Click on Done.	You return to the Configuration Manager window.

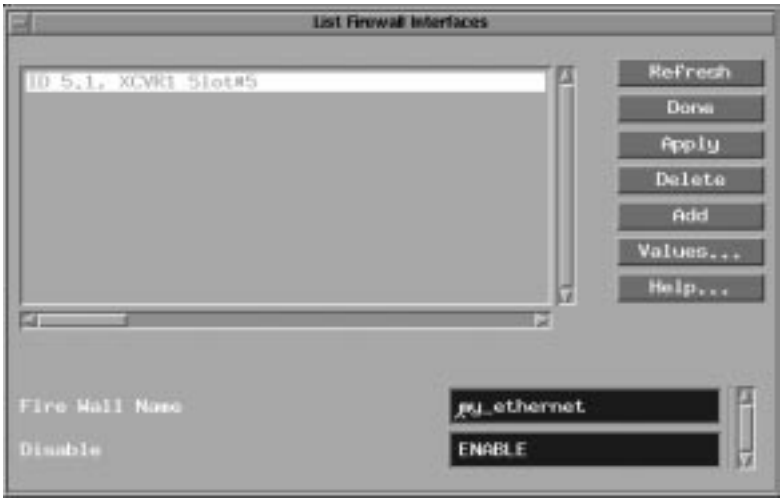

Figure 3-3. List Firewall Interfaces Window

Note: Once the firewall is protecting your router, if you put firewall protection on a new interface, the new interface will use the default security policy supplied by Check Point, which prevents the new interface from communicating with the router.

You can download your customized security policy to the new interface using the Check Point FireWall-1 command line interface. You can also use the Check Point FireWall-1 graphical user interface (GUI) to download the security policy. The GUI, however, downloads the same security policy to all interfaces. For further information and instructions, see your Check Point documentation.

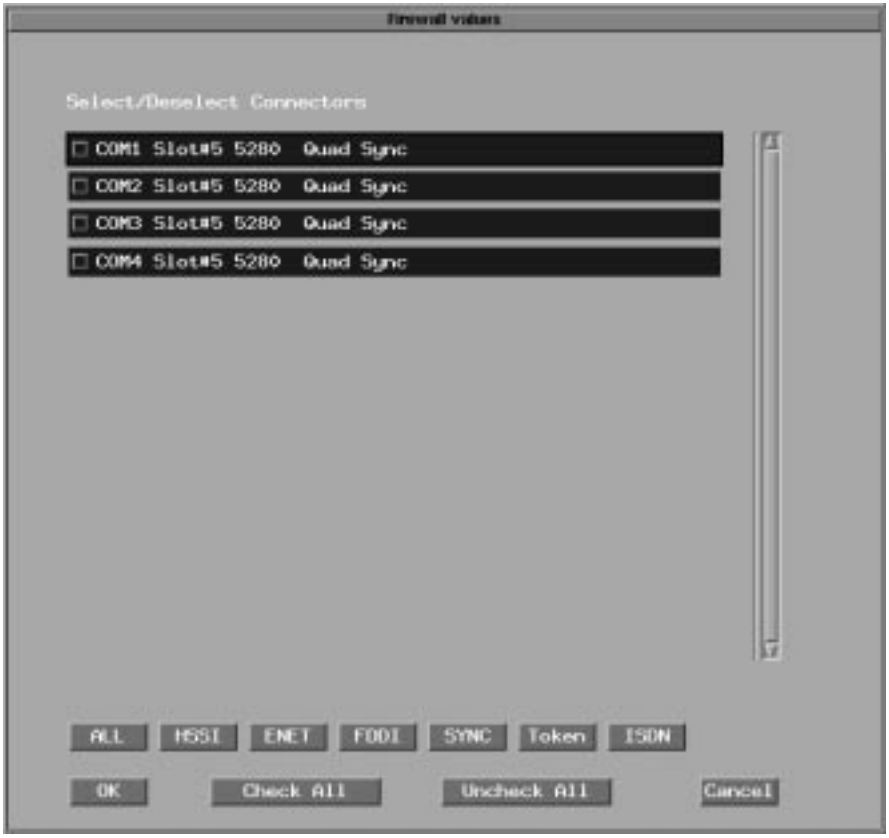

Figure 3-4. Values Window

Once you enable the firewall on an interface and reboot the router, you will not be able to communicate with the router through Site Manager until you change the FireWall-1 default security policy. For more information, see "Defining a Firewall Security Policy" on page 3-13.

Caution: If your firewall management station and router are on different subnets, you will not be able to communicate with the router from the management station unless you establish a static route from the management station to the router before you activate the firewall. For information about creating a static route, see *Configuring IP Services*.

Activating the Firewall

Before the FireWall-1 security policy can take effect on the router, you must first activate the firewall by booting the router using Site Manager on the management station. Booting a router warm-starts every processor module in the router. Pressing the Reset button on the front panel of the router performs the same procedure.

Note: When you activate the firewall, the default security policy prevents all interfaces supported by the firewall from communicating with the router. If the firewalled router and management station are on different subnets, you must establish a static route to enable communication between the router and the management station before you activate the firewall. For information about configuring a static route, see *Configuring IP Services.*

To reboot the router using Site Manager:

1. **From the main Site Manager window, choose Administration > Boot Router.**

   The Boot Router window opens (Figure 3-5).

Figure 3-5. Boot Router Window

2. **Specify the correct volume and boot image.**
3. **Select the correct router volume and configuration file. Then click on Boot.**

   A confirmation window appears.

4. **Click on OK in the confirmation window and wait a few minutes to give the router time to reboot.**
5. **Choose View > Refresh Display from the main Site Manager window to verify that the router booted correctly.**

If the router booted correctly, system information appears in the main Site Manager window.

If the router did not boot correctly, system information does not appear. In this case, make sure that you followed the procedures described in this section.

If you have any questions, refer to *Configuring and Managing Routers with Site Manager* or call your local Bay Networks Technical Solutions Center.

Defining a Firewall Security Policy

A *security policy* is a collection of rules that define the way the firewall operates. The default FireWall-1 security policy drops all attempts at communication with the router. This security policy goes into effect when you first activate the firewall on the router.

You must establish a security policy that explicitly defines acceptable communication to the router, based on the source address, destination address, and type of service. For details about how to configure a security policy, see your Check Point FireWall-1 documentation.

Installing the Security Policy on the Router and Its Interfaces

Once you have defined a security policy, you must install it on the router. Installing a security policy means downloading it to the firewalled objects that will enforce it.

When you download the security policy, the FireWall-1 software:

- Verifies that the rule base is logical and consistent
- Generates an inspection script from the rule base
- Compiles the inspection script to generate inspection code for the router
- Downloads the inspection code to the router

Note: Once the firewall is protecting your router, if you put firewall protection on a new interface, the new interface will use the default security policy supplied by Check Point, which prevents the new interface from communicating with the router.

You can download your customized security policy to the new interface using either the Check Point FireWall-1 command line interface or the Check Point FireWall-1 graphical user interface (GUI). The GUI, however, downloads the same security policy to all interfaces.

For instructions on how to install the security policy, see your Check Point FireWall-1 documentation.

Deleting Firewall from the Router

You can use either Site Manager or the Technician Interface to delete a firewall from the router. Deleting a firewall using Site Manager does not affect internal resources that were originally allocated for the FireWall-1 application. To dynamically delete a firewall from the router *and* free up internal resources allocated for the FireWall-1 application, you must use the Technician Interface.

Deleting Firewall Locally or Remotely Using Site Manager

Site Manager allows you to delete a firewall from the entire router in local and remote modes only.

To delete a firewall:

Site Manager Procedure	
You do this	**System responds**
1. From Configuration Manager, choose **Platform**.	The Platform menu opens.
2. Choose **FireWall**.	The FireWall menu opens.
3. Choose **Delete**.	A dialog box opens, asking if you are sure that you want to delete the firewall.
4. Click on **OK**	You return to the Configuration Manager window.

Warning: Deleting a firewall using Site Manager deletes the firewall management information base (MIB). This action disables firewall functionality on the router, but it does not affect internal resources that were originally allocated for the FireWall-1 application.

After you delete a firewall using Site Manager, you should save the configuration file and reboot the router to free internal resources. You can then reconfigure FireWall dynamically.

Deleting Firewall Dynamically Using the Technician Interface

To delete a firewall dynamically, you must use the Technician Interface. The Technician Interface allows you to delete a firewall on a slot/port basis, or from all ports on the router.

firewall delete [<*slot*> <*port*> | **_all**]

slot port	Identifies the location of the firewall to be deleted.
_all	Specifies to delete all instances of the firewall from the router.

Warning: The **firewall delete all** command deletes the MIB. This action disables the FireWall functionality on the router, but it does not affect internal resources that were originally allocated for the FireWall-1 application.

After using the **firewall delete all** command, you should save the configuration file and reboot the router to free internal resources. You can then reconfigure FireWall dynamically.

Troubleshooting Checklist

If you experience problems with FireWall-1, verify that you have performed these steps:

- Enabled IP on the router
- Enabled TCP on all slots on the router
- Created a firewall using Site Manager
- Created a static route if the router and firewall management stations are on different subnets
- Synchronized the router and management station passwords by executing the **fwputkey** command on both the router and the firewall management station
- Defined a security policy and added a network object for the router using the FireWall-1 graphical user interface
- Saved the configuration and booted the router
- Installed the security policy on the router

If you have performed these steps and are still having system problems, contact your Bay Networks Technical Solutions Center.

Appendix A
Parameter Descriptions

This appendix contains parameter descriptions for BaySecure FireWall-1 parameters.

FireWall Enable Parameter

Parameter: Enable

Path: **Platform > FireWall > Global**

Default: Enable

Options: Enable | Disable

Function: Enables or disables the firewall on the entire router.

Instructions: Choose Enable to allow the firewall to be active on the router. Choose Disable to disable the firewall on the router.

FireWall Parameters

Parameter: **Log Host Address**

Path: **Platform > FireWall > FireWall Parameters**

Default: 0.0.0.0

Options: Any valid IP address.

Function: Identifies the IP address of the primary firewall management station.

Instructions: Enter the IP address of the PC or UNIX workstation where you installed the Check Point FireWall-1 management software. If you have installed FireWall-1 management software on more than one PC or UNIX workstation, enter in the IP address of the workstation you plan to use as your primary FireWall-1 management station.

If the IP address of the management station and the IP address of the router are on different subnets, then you must configure a static route to the router to enable communication between the router and the management station. *Configuring IP Services* provides information about configuring a static route.

Parameter: **Log Host Backup 1**

Path: **Platform > FireWall > FireWall Parameters**

Default: 0.0.0.0

Options: Any valid IP address.

Function: Identifies the IP address of the first backup firewall management station.

Instructions: Enter the IP address of the PC or UNIX workstation where you installed the Check Point FireWall-1 management software. If you have installed FireWall-1 management software on more than one PC or UNIX workstation, enter in the IP address of the workstation you plan to use as your first backup FireWall-1 management station in the event that the primary management station loses communication with the router.

If the IP address of the management station and the IP address of the router are on different subnets, then you must configure a static route to the router to enable communication between the router and the management station. *Configuring IP Services* provides information about configuring a static route.

Parameter: **Log Host Backup 2**

Path: **Platform > FireWall > FireWall Parameters**

Default: 0.0.0.0

Options: Any valid IP address.

Function: Identifies the IP address of the second backup management station.

Instructions: Enter the IP address of the PC or UNIX workstation where you installed the Check Point FireWall-1 management software. If you have installed FireWall-1 management software on more than one PC or UNIX workstation, enter in the IP address of the workstation you plan to use as your second backup FireWall-1 management station in the event that the primary and first backup management stations lose communication with the router.

If the IP address of the management station and the IP address of the router are on different subnets, then you must configure a static route to the local host IP address to enable communication between the router and the management station. *Configuring IP Services* provides information about configuring a static route.

Parameter: **Local Interface IP Address**

Path: **Platform > FireWall > FireWall Parameters**

Default: 0.0.0.0

Options: Any valid IP address.

Function: Identifies the IP address of the router to be protected by the firewall.

Instructions: Enter the IP address of the router you intend to have protected by the firewall.

If the IP address of the firewall management station and the IP address of the router are on different subnets, then you must configure a static route to the local host IP address to enable communication between the router and the firewall management station. *Configuring IP Services* provides information about configuring a static route.

List FireWall Interfaces Parameters

Parameter: **Name**

Path: **Protocols > IP > FIREWALL**
Default: None
Options: Any string of alphanumeric characters.
Function: Identifies an interface by name.
Instructions: Enter a meaningful name in alphanumeric characters.

Parameter: **Disable**

Path: **Protocols > IP > FIREWALL**
Default: Disable
Options: Enable | Disable
Function: Enables or disables the firewall on one or more interfaces.
Instructions: Highlight one or more interfaces and choose Enable to allow the firewall to be active on the interfaces. Choose Disable to deactivate the firewall on the interfaces.

Index

A

acronyms, xi

activating FireWall-1, 3-12

adding
- administrators, 2-18
- groups, 2-18
- GUI clients, 2-12, 2-18
- license, 2-12, 2-18
- remote modules, 2-12, 2-18

B

backup management station, 3-6, 3-7

booting the router, 3-12

C

Check Point, contacting, 2-2, 2-4

commands
- commit, 3-2
- fw putlic, 2-19
- fwconfig, 2-18
- fwfilex, 2-20
- fwinstall, 2-14
- fwputkey, 2-19
- fwstart, 2-19
- fwstop, 2-19
- fwui&, 2-20
- set, 3-2

Configuration Manager, 3-2

configuring a firewall, 3-1

creating a firewall, 3-1

D

daemons, 2-19

E

educational services, xii

enabling the firewall
- on an interface, 3-8

extracting tar files, 2-13

F

file transfer, 2-20

FireWall-1 License
- for the Management station, obtaining, 2-1
- for the router, obtaining, 2-1

fw putlic command, 2-19

fwconfig command, 2-18

fwfilex command, 2-20

fwinstall command, 2-14

fwputkey command, 2-19

fwstart command, 2-19

fwstop command, 2-19

fwui& command, 2-20

G

groups, adding, 2-18

GUI clients, adding, 2-12, 2-18

I

inspection code, 3-14

installation
- options, 2-14
- sample, 2-6, 2-14

installing management software, 2-14

L

license
adding, 2-12, 2-18
installing on management station, 2-19

M

management station, 3-4
primary, 3-5
secondary, 3-6
tertiary, 3-7
modules
firewall stateful inspection, 1-2
mounting a CD drive, 2-13

P

product support, xii
publications, Bay Networks, xi

R

refreshing the display, 3-13
remote modules, adding, 2-12, 2-18
Reset button, 3-12
rule base, verifying, 3-14

S

security policy
configuring, 3-13
downloading, 3-14
security rules, 3-13
serial number, obtaining, 2-2, 2-4
starting the daemons, 2-19
stateful inspection module, 1-2
static route, configuring, 3-12
support, Bay Networks, xii
synchronizing the router and management station, 2-19

T

tar files, extracting, 2-13
technical publications, xi
technical support, xii
Technician Interface, 3-2
transferring files, 2-20